SCANNERS AND THE LAW: A CHRONOLOGY

by Bob Grove, President, Grove Enterprises; Publisher, Monitoring Times

1934 **Congress passes the Communications Act,** establishing the Federal Communications Commission (FCC), and includes the visionary Section 605 which addresses the inevitability of interception of radio signals, but prohibits the disclosure of the contents of such transmissions, or the use of their contents for personal gain. (Exhibit A)

1986 **Congress passes the Electronic Communications Privacy Act (ECPA),** for the first time censoring Americans' historic right to the airwaves by forbidding listening in on several types of radio signals, including the radio portion of a telephone conversation. (Exhibit B)

The Cellular Telecommunications Industry Association (CTIA) issues public statements that it will soon offer digital encryption systems to provide their customers privacy. 11 years later, these privacy systems are only in an estimated 10-20% of the cellular market.

1989 **Two prominent CTIA members,** Uniden and Radio Shack, **discontinue manufacturing** several scanner models with cellular frequency coverage, although follow-on models are easily restorable. Other manufacturers continue to offer cellular frequency coverage since existing law forbids listening, not manufacture. Many companies perform cellular restoration at the time of sale so that the censored scanners will have the same frequency coverage as perfectly legal, competitive models.

1990 **CTIA and the Telecommunications Industry Association (TIA) adopt the IS-54 standard** for digital voice cellular encryption, called Time Division Multiple Access (TDMA). A secondary standard, Code Division Multiple Access (CDMA) is also proposed.

1992 **President Clinton signs the Telephone Disclosure and Dispute Resolution Act (TDDRA),** directing its implementation in 1994, but which contains no reference to radio scanners.

1993 **The TDDRA is altered** with a last-minute Cellular Amendment just before Congressional adjournment, allowing little legislative scrutiny, and averting public awareness or comment, but banning the importation or manufacture of scanners capable of receiving, or being readily altered to receive, cellular telephone frequencies. (Exhibit C)

In response to an enormous outcry from concerned citizens, **Bob Grove tiles formal commentary with the FCC** and asks to give testimony to the House Subcommittee to cite 20 potentially disabling aspects of the Cellular Amendment to the pending TDDRA. (Exhibit D) Access to the Subcommittee is denied, but Grove is allowed to come to Washington to talk with a Congressional aide and leave his petition. No further response was forthcoming from the Subcommittee. Grove publishes for public comment the list in the magazine, *Monitoring Times.* Public response was considerable.

The FCC issues Report to Congress on "Available Security Features For Providing Cellular Telephone Privacy," describing several voice encryption systems available to the cellular industry. (Exhibit E)

1994 **Congress implements the TDDRA**

Illinois Attorney General Roland Burris issues a formal opinion that, under Illinois state law, eavesdropping on cellular and cordless telephones is legal because there is "no reasonable expectation of privacy." CTIA issued a public objection. (Exhibit F)

Kenneth *Vito Zichi*
3018 Moyer Road
Williamston, MI 48894-9506

Radio Listening and the Law

"Unlike many hobbies, shortwave listening has relatively few laws that restrict its afficionados. In fact, barring the illegality of using a receiver as a murder weapon, the one law that has any direct bearing on the shortwave listener is the so-called 'secrecy law'."

When Mel Hickman wrote that in 1973, he was right. Today, however, there are other laws radio listeners must contend with_

Many states have laws restricting the use of scanners or other police band radios in moving vehicles, and in certain other &cumstances. Unfortunately, the variety and number of such state laws make a comprehensive look at them impractical for this column.

Whatwewilldoislookatthemainpointsof the two major federal laws regulating radio listening: the "secrecy law" (The Communications Act of 1934, #705) referred to above, and the recently amended Electronic Communications Privacy Act (ECPA).

The Secrecy Law ~

The secrecy law, technically known as 47 USCS #605, was first enacted in June of 1934, and last amended in Oaober of 1984. (You may also see it referred to as the Communications Act of 1934, Title VII, #705). Its purpose from the beginning was to provide those using the radio to transmit private messages with a measure of security by making it illegal to disclose the contents of a transmission to anyone other than the intended party.

Nothing in this law restricts listening to private communications, only the listening *and disclosure* of such transmissions. Thus, it comes into play only when a listener attempts to verify (QSL) a nonbroadcast station. But in order to fully understand the law, you unfortunately will have to read it, and for Congress' purple prose, I apologize in advance!

> (a)Except as authorized by chapter 119, title 18 United States Code [18 USCS ##2510 et seq.-the ECPA], no person receiving, assisting in receiving, transmitting, or assisting in transmitting any interstate or foreign communications by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof.... (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination...(5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the aistence, contents, substance, purport, effect or meaning of such intercepted communications to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communications was intercepted, shall divulge or publish the existence, content, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.
>
> (d)(1)Any person who willfully violates subsection (a) shall be fmed not more than $1.000 or imprisoned for not more than 6 months, or both.
>
> (2)Any person who violates subsection (a) willfully and for purposes of direct or indirect commercial advantage or private financial gain shall be fmed not more than $25,000 or imprisoned for not more than 1 year, or both, for the first such conviaion and shall be fined not more than $50,000 or imprisoned for not more than 2 years, or both, for any subsequent conviction.
>
> (3) [provisions for civil litigation based on this section and providing for remuneration of any damages suffered]

As a note. Congress uses the word "intercept' *to* mean "receive", not what you wuld expect from the common meaning of the wrd

The details are there if you care to wade through the language, but in a somewhat oversimplified nutshell, #605 provides that a listener may not divulge the content *or even the existence* of a two-party transmission, except for distress calls, and ham and CB transmissions. Similarly, a listener receiving such transmissions may not use the information gleaned for his own benefit. In other words, while it is OK to listen to anything you want, you cannot, for example, send a reception report to a Coast Guard station disclosing you heard it while it was handling traffic. Even if you do not mention the name of the ship it was in contact with, or what was said, the mere *existence* of the transmission may not be disclosed. Under the law, such a report would be improper, since it would "benefit" a person other than the intended addresseee, namely, the listener seeking the QSL.

On the other hand, if you waited until the Coast Guard station began reading the maritime weather report or the latest Notice to Mariners, and submitted a report on that transmission you would be doing nothing illegal, since the transmission was not meant for anyone in particular. It falls under the "communication transmitted by a station for the use of the general public' exception.

This law was meant to allow people using radio for private or semi-private communications some assurance that their words would not become front-page news, and was never intended to insure "privacy" in the absolute sense of that word. This purpose is acknowledged in the case entitled "Re Roberts Flying Service, Inc,, a al." [30 FCC2d 823 (1971)]. Although that case attempts to say #605 does prohibit listening alone, it concludes by saying that the section does not protect the expectation of "full privacy" but only the user's expectation that his communication will not become "generally public" or used to his detriment.

However, the way this section has been interpreted specifically aduda a situation that the framers of the US Constitution would have been concerned about if radio had been around in 1788: reception and use of transmissions by police and other government officers, and the "unreasonable search"

ramifications of a policeman listening in, for example, on your wireless telephone. Title 18 of the US Code, and specifically the ECPA, covers such Fourth Amendment concerns.

Contrary to the impression *many radio* hobbyists have, the ECPA actually is designed to set forth circumstances when it is alright to "intercept" a communication - thus the reference to it in the Secrecy Law. The basic purpose behind Title 18 originally was to flesh out the requirements of the Fourth Amendment securities, and provide guidance to police and other officials about what constitutes proper behavior within the Constitution.

However, in the process of telling us - and the police - when it is OK to receive electronic signals (like when you have a search warrant issued with probable cause) the ECPA also tells us that under any other circumstances it is not OK to listen in on others' transmissions.

But that is getting ahead of the story. The ECPA, technically, 18 USCS #2510 et.seq. was first enacted in June of 1968, and dealt only with wire and oral communications. In 1986 it was modified by Congress to also include radio communications, and the name of the law was changed to the ECPA to reflect that. The text relevant to radio listeners is in #2511:

> (1) Except as otherwise provided in this chapter any person who -
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept, endeavor to intercept, any wire, oral, or electronic communication...[(b) refers to oral communications only]
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the infotmation was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection: or
> (d) intentionally uses, or endeavors to use the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; shall be punished as provided in subsection (4) [which provides for fines and imprisonment for up to 5 years}...

Again, the way Congress uses "intercept" in this law also means "receive". Unfortunately, unlike the language of the secrecy law, Congress here did not use the phrase "and divulge" when describing what was prohibited Therefore, under the ECPA, merely listening to a transmission is, on it's face, illegal.

But all is not so grim. Congress realized that the language above, left to itself would make listening even to a broadcast station illegal, and thus was overly broad Subsection two goes on to list the exceptions to the general rule set out above.

> (2). . . (g) It shall not be unlawful under this chapter...for any person - (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such elecwnic communication is readily accessible to the public
> (iii to intercept any electronic communication which is transmitted -
> (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles or persons in distress;
> (II)by any government4 law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
> (IV) by any marine or aeronautical communications system...(or)
> (iv)to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference;

There is a sentence in those exceptions that I believe Congress did not fully appreciate: "It shall not be unlawful under this chapter...for any person...to intercept or access an electronic communication made through an eleo tronic communication system that is configured so that such electronic communication is readily accessible to the public."

To paraphrase tax specialists, that is a loop hole you can drive a truck through. In my interpretation, that phrase means if it is unencoded, you can listen to it. Period In fact, even if it is encoded, so long as you do not attempt to decode it without authorization, you can listen all you want. You are not intercepting the "communication" if you do so - you are only intercepting the transmission, which is something the ECPA does not address

Unfortunately, Congress certainly did intend to restrict what we could listen to via the mechanism of the ECPA. That intent was made painfully clear by discussions in committee when the law was passed, and it was revealed that based on the requests of cellular telephone manufacturers and others, Congress believed it appropriate to restrict the general public's ability to legally monitor two-party transmissions. Fortunately, the law as passed (and even as originally proposed) does not do what Congress set out to do!

In short, as presently written neither law discussed above prohibits hobbyists from listening to transmissions of any sort, provided that if they are encoded, the hobbyist cannot attempt to decode them without authorization. The Secrecy law does prohibit disclosure of the existence or content of certain transmissions, however, primarily to ensure some degree of privacy for the people using radio as a private communication medium. I believe that latter goal is appropriate - even though it does mean inconvenience for DXers seeking QSLs - given that radio is meant to be a useful technology.

I do not believe Congress is acting within the nation's best interest in attempting to prohibit *reception* of two-party transmissions, but that is a drum you will likely hear others beat. At any rate, the ECPA as *currently enacted* does not prohibit "unauthorized" monitoring of two-party communications

---

Kenneth Vito Zichi is a General Practice attorney admitted to pmctice in both Federal and State courts in Michigan. He is a graduate of the University of Michigan ***Law School, and a member of the Michigan Bar and Livingston County Bar Association, as well as the Amen'-con Bar Association and the Association of Trial Lawyers of America***

Exhibit B

ASSOCIATION RICAN RADIO CLUBS

Robert Horvitz
Government Affairs Liaison

1634 15th Street, NW
Washington, D.C. 20009

Telephone: (202) 232-3677

10 October 1986

Preliminary Analysis of the Electronic Communications Privacy Act

The Electronic Communications Rivacv Act of 1986 (ECPA) passed both Houses of Congress at the start of October. The-radio provisions of the ECPA go into effect 90 days after it is signed by the Resident - that is, sometime in mid-January, 1987. The final draft of the bill is printed in the October 1st issue of the Congressional Record, starting on page S-14441. Here is a preliminary analysis of the new law as it affects radio monitoring.

(Note: The Senate Judiciary Committee's report interpreting the ECPA has not yet been released. -Without that report, our analysis cannot be complete or definitive.)

* *

What the ECPA Does

The ECPA amends US Code Title 18, Chapter 119, the federal law governing the interception of "wire" and "oral" communications, to protect a new legal category, "electronic communication." It sets new rules for electronic surveillance by law enforcement agencies, and for investigative access to electronic mail and computer files. It also increases criminal penalties for malicious interference with satellite transmissions.

"Electronic communication" is defined as 'any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include-

(A) the radio portion of a cordless telephone communication...;
(B) any wire or oral communication;
(C) an; communication made through a tone-only gaging device; or
(D) an communication from a tracking device...

Radio and wire transmissions are thus merged in this new term. However, the new law also retains and adapts the earlier legal definition of "wire communication" as a category separate from 'electronic communication." "Wire communication' now means voice telephony, regardless of whether transmission is by wire or radio. The term "oral communication" is clarified to exclude voice transmissions by wire, radio or other electronic means. In other words, non-voice communications by wire are considered "electronic' communications, as are communications by radio which do not involve telephone transmission.

Unauthorized interception of the radio portion of a "wire" or "electronic" communication carries lesser penalties than does interception of the wire segment of the same communication – if it's not for an illegal, commercial or "tortious" [lawsuit-susceptible] purpose. See the 'Penalties" section, below, for details.

What May Legally be Monitored

* Any marine or aeronautical radio communication
* Any Amateur, CB or General Mobile Radio Service transmission
* Any communication transmitted 'for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress"
* The radio portion of cordless telephone communications linking the handset and base unit
* Tone-only paging signals
* Certain types of audio subcarriers (to be specified in Senate report)
* Signals causing harmful interference to "any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference'
* Satellite transmissions of 'network feeds,' some audio subcarriers, and cable programming covered by Section 705(b) of the Communications Act
* Any governmental, law enforcement, civil defense, private land mobile, or public safety (including police and fire) radio communications system which is 'readily accessible to the general public'
* Any other electronic communication made through a system 'configured so that such electronic communication is readily accessible to the general public'

In most cases, radio communications defined as NOT 'readily accessible' will be illegal to monitor, unless one of the above exemptions applies. "Readily accessible to the general public" is defined to mean that the communication is NOT:

- scrambled or encrypted;
- 'transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication' [the House report says this means spread-spectrum signals];
- 'carried on a subcarrier or other signal subsidiary to a radio transmission;"
- "transmitted over a communication system provided by a common carrier' (except for tone-only paging signals);
- transmitted on frequencies allocated under FCC rules part 25 [communication-relay satellites]; part 74(D) [remote broadcast pick-up stations]; part 74(E) [aural broadcast auxiliaries, including studio-to-transmitter links]; part 74(F) [television broadcast auxiliaries & studio-to-transmitter links]; or part 94 [private fixed microwave].

As mentioned above, some exceptions override the general ban on reception of allegedly "inaccessible" signals. For example, the radio emissions of a cordless phone may be monitored, even though it relays common carrier communications.

Similarly, marine and aeronautical radiotelephone signals are legal to monitor. (In contrast, phone-patches in the 800 MHz Specialized Mobile Radio service are legally protected, since the phrase "readily accessible' qualifies the exception for private land mobile radio, which includes SMRs.)

The forthcoming Senate report on the ECPA is expected to identify types of audio subcarriers that may legally be monitored, even though the new law declares all subcarriers to be 'inaccessible.' (Taken literally, that makes listening to FM stereo broadcasts, and the audio portion of TV broadcasts, federal crimes!)

Although broadcast remote pick-up (RPU) stations authorized under FCC part 74(D) are declared to be 'inaccessible," they operate near 26, 153, 161, 166, 170, 450 and 455 MHz, usually with city-wide audio coverage. Used by broadcasters to coordinate the coverage of events outside the studio, RPUs can be received on most scanners. Indeed they are favorites among scanner owners because of their newsgathering role. As a result of an amendment introduced by Sen. Paul Simon at ANARC's request, the ECPA creates no criminal liability in monitoring RPUs when the monitoring is for no bad purpose (but see next section for civil liabilities).

Penalties

For most unencrypted radio communications protected under the ECPA, intentional unauthorized interception carries a criminal penalty of up to one year in jail and/or a fine of up to $100,000 - for a first offense which is not for a bad purpose - i.e., 'not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain.'

If it is a 'public land mobile radio service' communication (i.e., a cellular or a traditional IMTS radiotelephone call), or any type of paging except for tone-only, and the signal is not scrambled or encypted, and if the interception is intentional but not for a bad purpose, the penalty for a first offense is a fine of up to $500.

If the communication is scrambled or encrypted, or the interception is for a bad purpose or is a second or subsequent offense, the penalty is up to 5 years in jail and/or a fine of up to $100,000.

Intentional interception of an unencrypted part 74(D) transmission, without bad purpose, carries no criminal penalties. However, the federal government may seek a court injunction against a specific interceptor, and assess civil damages of up to $500. Any violation of the injunction carries with it a mandatory $500 civil fine, liability for any actual damage suffered by the plaintiff, or statutory damages of up to $1000.

Any criminal violation of the ECPA exposes the interceptor to civil liabilities (risk of a lawsuit). For any violation other than those described in the last paragraph, courts may reclaim any profits made from or damages caused by the interception, or assess statutory damages of $100 for each day of violation, or $10,000, whichever is greater.

Intentional vs. Inadvertant

The ECPA makes it a federal crime to intentionally intercept, disclose or use electronic communications protected under this Act. Even "endeavors to intercept" are a crime [section 2511(l)(a)]. That is, merely trying to intercept a protected communication is a crime, even if you don't succeed! Under the ECPA, acting on the intention is sufficient to constitute a crime.

Obviously, the exact legal meaning of 'intentional" - and the kind of proof required to establish intent in court - are crucial. The House report says intentional means that acquiring the contents of an electronic communication is one's "conscious objective." According to the House report, requiring intent "precludes the application of civil or criminal liability for acts of inadvertant interception." [emphasis added] However, the report adds, "The term 'intentional' does not require that the act was committed for a particular purpose or motive," [emphasis added]

The ECPA thus does not criminalize an act so much as a "state of mind' or attitude relating to the act. Interception achieved by accident is not a crime. Unfortunately, this distinction is rather murky in the case of recreational scanning with a multiband radio receiver. Does casual browsing constitute intentional or inadvertant interception? what about automatic band searches? and what constitutes proof of intent - possession of a frequency list? We hope for answers to some of these questions in the Senate report. In any event, requiring proof of intent should limit a hobbyist's chances of being successfully prosecuted for recreational monitoring that causes no detectable harm to those whose radio communications were tuned in.

Surreptitious Interception Devices

An easy way to enforce the ECPA would be to criminalize ownership of devices capable of receiving protected communications. In fact, the ECPA amends sections 2512 and 2513 of US Code Title 18 in an attempt to do just that. When the new law goes into effect, it will become illegal to manufacture, assemble, possess, sell, advertise or send through the mail any electronic device whose design "renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.'

Due to imprecise drafting, the ECPA's ban on "surreptitious interception devices" does not distinguish between electronic communications that are legal to receive and those that are illegal. Depending on how the word 'surreptitious' is defined, a AM-FM broadcast receiver concealed in a stuffed animal could qualify as an illegal device; similarly, a microcomputer with a modem and built-in code-breaking software might constitute an illegal device, depending on how the word "primarily" is defined. We can only hope that the Senate report defines surreptitious interception devices in a way that is both clear and narrow. We also hope for insight into the new legal status of subcarrier tuners, voice inverters (simple descramblers), teletext readers, radioteletype terminals with bit-code translation features, and programmable scanners.

Before the
Federal Communications Commission
Washington, DC. 20554

ET Docket No. 93-1

In the Matter of

Amendment of Parts 2 and 15 to
Prohibit Marketing of Radio Scanners
Capable of Intercepting Cellular
Telephone Conversations

Exhibit C

NOTICE OF PROPOSED RULE MAKING

Adopted: January 4, 1993; Released: January 13, 1993

Comment Date: February 22, 1993
Reply Date: March 8, 1993

By the Commission.

INTRODUCTION

1. By this action, the Commission proposes to amend Parts 2 and 15 of its rules to prohibit the manufacture or importation of radio scanners capable of receiving frequencies allocated to the Domestic Public Cellular Radio Telecommunications Service.[1] This action is in response to the Telephone Disclosure and Dispute Resolution Act (Act), Pub. L. 102-556. The proposed rules are intended to increase the privacy protection of cellular telephone users without unduly restricting legitimate uses of scanners.

BACKGROUND

2. The Domestic Public Cellular Radio Telecommunications Service ("Cellular Radio Service") provides telephone service to mobile customers. Cellular telephones use frequencies in the bands 824-849 MHz and 869-894 MHz to connect their users to other cellular system users and to the Public Switched Telephone Network.

3. As defined within our rules scanning receivers or "scanners," are radio receivers that automatically switch between four or more frequencies anywhere within the 30-960 MHz band.[2] In order to control their potential to cause harmful interference to authorized radio communications, the rules require that scanners receive an equipment authorization (certification) from the Commission prior to marketing.[3] The Electronic Communications Privacy Act of 1986, Pub. L. 99-508, in part, made it illegal to intentionally intercept cellular communications or to manufacture equipment primarily useful for the surreptitious interception of cellular communications.[4] However, the Commission was not given specific authority to deny equipment authorization to scanners that receive cellular frequencies. As a result, scanners capable of receiving cellular frequencies are routinely authorized by the Commission.

4. In the past few years, 22 different models of scanning receivers capable of receiving cellular telephone transmissions have been issued grants of equipment authorization. During this same period, ten other models capable of tuning frequencies between 806 and 900 MHz *except* for the cellular bands have also been authorized. Several publications currently on the market describe relatively simple modifications that users can make to many of the latter tuning receivers to enable that equipment to receive cellular telephone transmissions.

5. On October 28, 1992, the President signed the Telephone Disclosure and Dispute Resolution Act into law. Section 403 of this Act amends the Communications Act of 1934 (47 U.S.C. Section 302) by requiring that by April 26, 1993 (180 days after enactment of the Act), the Commission prescribe and make effective regulations denying equipment authorization for any scanning receiver that is capable of

- receiving transmissions in the frequencies allocated to the domestic cellular radio service,
- readily being altered by the user to receive transmissions in such frequencies, or
- being equipped with decoders that convert digital cellular transmissions to analog voice audio.

Further, new Section 302(d)(2) provides that, beginning one year after the effective date of the regulations adopted pursuant to paragraph (d)(1), no receiver having such capabilities shall be manufactured in the United States or imported for use in the United States.[5]

DISCUSSION

6. In accordance with Section 403 of the Act, we are proposing to deny equipment authorization to scanning receivers that tune frequencies used by cellular telephones. We are also proposing to require applicants for the authorization of scanning receivers to include in their applications a statement declaring that their receivers cannot be tuned to receive cellular telephone transmissions.

7. Developing regulations that deny equipment authorization to scanning receivers capable of "readily being altered by the user" to receive cellular telephone transmissions is somewhat more complicated. Most of the alterations that users can readily accomplish are possible because the microprocessor chips that control the tuning circuitry of many scanning receivers are designed to receive cellular telephone transmissions. Many scanners are

[1] The Commission's regulations regarding the Domestic Public Cellular Radio Telecommunications Service are set forth in Part 22 of the FCC rules, 47 CFR Part 22, Subpart H.

[2] *See* 47 CFR Section 15.3(v).

[3] *See* 47 CFR Sections 15.101(a) and 2.1031 *et seq.*

[4] *See* 18 U.S.C. Sec. 2511, 2512.

[5] *See* Telephone Disclosure and Dispute Resolution Act, *supra*., Section 403. Section 403 also requires that the Commission report to Congress, by June 1, 1993, on available security features for both analog and digital cellular radio signals. This reporting requirement will be dealt with separately from this proceeding.

marketed worldwide. and some countries do not prohibit scanning of the 824-849 MHz and 869-894 MHz bands. Prior to marketing one of these receivers in the United States, the manufacturer can choose to defeat the ability to receive cellular transmissions by adding a simple component such as a resistor, diode or jumper wire to the receiver's printed circuit board. In order to restore cellular coverage, the user simply has to remove the component that was added to block out this coverage. It is clear from the legislative history of the Telephone Disclosure and Dispute Resolution Act that Congress intended the Commission to craft rules that preclude such simple modifications.[5]

8. We are proposing to require that scanning receivers be incapable of being readily altered by the user to operate within the cellular bands. To assist us in determining whether a scanner complies with this requirement, we propose to require applicants for scanning receive: equipment authorization to include in their applications a statement pledging that their receivers cannot be readiiy altered to receive cellular telephone transmissions. We also propose to prohibit the authorization of any scanning receiver for which cellular coverage can be restored by cutting, or adding, a simple component such as a resistor, diode or jumper wire, or for which cellular coverage can be restored by unplugging a semiconductor chip and/or plugging in a new one. We solicit comment on this proposed reporting requirement and on the definition of "readily altered." We also seek comment on whether additional information, such as why the receiver cannot be readily altered, should be required.

9. In compliance with the requirements of the Telephone Disclosure and Dispute Resolution Act, we propose to deny equipment authorization to any scanning receiver that can be equipped with decoders that convert digital cellular transmissions to analog voice audio. We invite comment on the potential impact of this requirement on existing models of scanning receivers.

10. There currently are a number of frequency converters on the market that convert cellular radio transmissions in the 800 MHz band to lower frequencies. These devices can be used in conjunction with scanners that receive frequencies below 800 MHz to enable the reception of cellular telephone transmissions. To allow such converters to be marketed would be inconsistent with the intent of the Act. Accordingly, we are proposing to deny equipment authorization to converters that tune, or can be readily altered by the user to tune, cellular telephone frequencies.[6] We will require that applicants for FCC equipment authorization of frequency converters used with scanners include in their applications a statement pledging that the converters cannot be easily altered to enable a scanner to receive cellular transmissions. We seek comment as to whether this statement should also include evidence indicating why the converter cannot be easily modified.

11. Under the rules we are proposing, if the Commission discovers evidence that a scanning receiver, or a frequency converter used with a scanning receiver, can be readily altered to tune cellular frequencies after it has received a grant of equipment authorization, the Commission will consider whether one grant should be revoked, and whether the manufacturer(s), importer(s), wholesaler(s) and retailer(s) of the receiver should be subject to enforcement action for violating Section 302 of the Communications Act of 1934, as amended, and the Commission's rules.[7]

12. The proposed rules are shown in Appendix A. The relevant text of the Telephone Disclosure and Dispute Resolution Act is shown in Appendix B.

PROCEDURAL MATTERS

13. *Initial Regulatory Flexibility Analysis.* Pursuant to the Regulatory Flexibility Act of 1980, 5 U.S.C. 603, the Commission's initial analysis is as follows:

I. *Reason for Action:* The Telephone Disclosure and Dispute Resolution Act requires this action to be taken.

II. *Objective:* The objective of the proposed rules is to help ensure the privacy of participants in cellular telephone conversations by significantly reducing the availability of scanning receivers that can be used to eavesdrop on these conversations.

III. *Legal Basis:* Action is proposed in accordance with Sections 4(i), 302(d), 303(f), 303(g) and 303(r) of the Communications Act of 1934, as amended, and Pub. L. 102-556.

IV. *Description, potential impact and number of small entities affected:* The proposed changes in the regulations would likely affect fewer than 50 small entities. Manufacturers of scanning receivers, or frequency converters used with scanning receivers, that can receive, or be easily altered to receive, cellular telephone transmissions would be required to modify their designs. These manufacturers would also be required to provide written statements indicating that their devices cannot be easily altered when they submit applications for equipment authorization. This would result in some expense to manufacturers.

V. *Any significant alternative minimizing the impact on small entities and consistent with the stated objectives:* None

---

[5] *See Congressional Record - Senate*, October 9, 1992, at S17121.

One obvious way to address these requirements is to require scanning receiver manufacturers to design microprocessor chips that are not capable of tuning cellular transmissions in the first place. This solution could increase the cost, at least in the short term, of bringing new scanning receivers to market because microprocessor chips would have to be redesigned. We recognize that this solution might not be effective if replacement microprocessors were on line or market that could be easily switched with the original microprocessor in order to restore cellular coverage. We seek comment on whether we should adopt regulations that require that no semiconductors in scanners be installed in sockets or that prohibit certain microprocessor models.

[6] These converters are receivers subject to authorization under the notification procedure. *See* 47 CFR Section 15.101. We are not proposing to subject cable television converters, or similar devices that may be capable of tuning to cellular frequencies, to these requirements.

[7] Sanctions may include administrative fines of up to $100,000 for each violation or for each day of a continuing violation, up to a total of $375,000. They may also include federal court civil seizure and forfeiture of the non-compliant equipment in question and/or issuance of a federal court injunction against further violations; and/or criminal penalties, upon conviction of a criminal fine of up to $100,000 for individuals, $200,000 for organizations, and/or imprisonment, for individuals, for up to one year or more. *See* 47 U.S.C. 501 and 503; and 18 U.S.C. 1512 and 3571.

14. *Comment Dates.* Pursuant to applicable procedures set forth in Sections 1.415 and 1.419 of the Commission's Rules. 47 CFR Sections 1.415 and 1.419, interested parties may file comments on or before **February 22. 1993. and reply comments on or before March 8, 1993.** These abbreviated comment periods are necessary to comply with the requirements in the Telephone Disclosure and Dispute Resolution Act. and are unlikely to be extended. To file formally in this proceeding, you must file an original and four copies of all comments. reply comments. and supporting comments. If you want each Commissioner to receive a personal copy of your comments, you must file an original plus nine copies. You should send comments and reply comments to Office of the Secretary. Federal Communications Commission. Washington. DC 20554 Comments and reply comments will be available for public inspection during regular business hours in the *dockets* Reference Room of the Federal Communications Commission. 1919 M Street. N.W., Washington. DC 20554.

15. *Ex Parte Rules - Non-Restricted Proceeding.* This is a non-restricted notice and comment rule making proceeding. *Ex parte* presentations are permitted. except during rhe Sunshine Agenda period. provided they are disclosed as provided in Commission rules. See *generally* 47 CFR Sections 1.1202. 1.1203 and 1.1206(a).

16. For further information on this proceeding contact David Wilson. Technical Standards Branch. Office of Engineering and Technology. X2-653-8 138.

FEDERAL COMMUNICATIONS COMMISSION

Donna R. Searcy
Secretary

APPENDIX A

Part 2 of Title 47 of the Code of Federal Regulations is proposed to be amended as follows:

PART 2–FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS: GENERAL RULES AND REGULATIONS

1. The authority citation for Part 2 continues to read as follows.

AUTHORITY: Sec. 4, 302, 303 and 307 of the Communications Act of 1934, as amended. 47 U.S.C. 154, 154(i), 302, 303, 303(r) and 307.

2. Section 2.975 is amended by adding a new paragraph (a)(8) to read as follows:

Section 2.975 Application for notification.

(a) * * *

(8) Applications for the notification of receivers contained in frequency converters used with scanning receivers shall be accompanied by an exhibit indicating compliance with the provisions of Section 15.121 of this Chapter.

3. Section 2.1033 is amended by adding a new paragraph (b)(12) to read as follows:

Section 2.1033 Application for certification

(b) * * *

(12) Applications for the certification of scanning receivers under Part 15 shall be accompanied by an exhibit indicating compliance with the provisions of Section 15.121 of this Chapter.

* * * * *

Part 15 of Title 47 of the Code of Federal Regulations is proposed to be amended as follows

PART 15–RADIO FREQUENCY DEVICES

1. The authority citation for Part 15 continues to read as follows:

AUTHORITY: Sec. 4. 302, 303 and *307 of* the Communications Act of 1934. as amended. 47 U.S.C. 154, 302, 303 and 307.

2. Section 15.37 is amended by revising paragraph (b) and adding a new paragraph (f), to read as follows:

Section 15.37 Transition provisions for compliance with the rules.

* * * * *

(b) * * * In addition, receivers are subject to the provisions in paragraph (f) of this Section.

* * * * *

(f) The manufacture or importation of scanning receivers, and frequency converters used with scanning receivers that do not comply with the provisions of Section 15.121 of this Part shall cease on or before April 26 1994. Effective April 16, 1993, the Commission will not accept applications for equipment authorization for receivers that do not comply with the provisions of Section 15.111 of this Part. This paragraph does not prohibit the sale or use of authorized receivers manufactured in the United States or imported into the United States, prior to April 26, 1994.

3. Section 15.121 is added to read as follows

Section 15.121 Scanning receivers and frequency converters used with scanning receivers.

Scanning receivers, and frequency converters used with scanning receivers, must be incapable of operating (tuning), or readily being altered by the user to operate, within the frequency bands allocated to the Domestic Public Cellular Radio Telecommunications Service. Receivers capable of "readily being altered by the user" include, but are not limited to, those for which the ability to receive transmissions in the restricted bands can be added by clipping the leads of, or installing, a diode, resistor and/or jumper wire or replacing a plug-in semiconductor chip. Scanning receivers, and frequency converters used with scanning receivers, must also be incapable of converting digital cellular transmissions to analog voice audio.

APPENDIX B

Section 403 of the Telephone Disclosure and Dispute Resolution Act (Pub. L. 102-556, enacted October 28, 1992)

Sec. 403. INTERCEPTION OF CELLULAR TELECOMMUNICATIONS

(a) AMENDMENT -- Section 302 of the Communications Act of 1934 (47 U.S.C. 302) is amended by adding at the end the following new subsection:

"(d)(1) Within 180 days after the date of enactment of this subsection, the Commission shall prescribe and make effective regulations denying equipment authorization (under part 15 of title 47, Code of Federal Regulations, or any other part of that title) for any scanning receiver that is capable of--

"(A) receiving transmissions in the frequencies allocated to the domestic cellular radio telecommunications service;

"(B) readily being altered by the user to receive transmissions in such frequencies; or

"(C) being equipped with decoders that convert digital cellular transmissions to analog voice audio.

"(2) Beginning 1 year after the effective date of the regulations adopted pursuant to paragraph (1), no receiver having the capabilities described in subparagraph (A), (B), or (C) of paragraph (1), as such capabilities are defined in such regulations, shall be manufactured in the United States or imported for use in the United States."

(b) REPORT TO CONGRESS -- The Commission shall report to Congress not later than June 1, 1993, on available security features for both analog and digital radio signals. This report shall include a study of security technologies currently available as well as those in development. The study shall assess the capabilities of such technologies, level of security afforded, and costs with wide-spread deployment of such technologies.

(c) EFFECT ON OTHER LAWS -- This section shall not affect section _____(2) of title 18, United State.; Code

Exhibit D

CONCENSUS OF OPPOSITION TO CELLULAR AMENDMENT TO THE FCC FUNDING BILL OF 1992

Prepared by Robert B. Grove
Publisher, Monitoring Times
November 14, 1991

There are more than 10 million scanner listeners in the United States. They agree that everyone is entitled to privacy when it can be reasonably expected, but are dismayed that their legislators passed the unenforceable and seriously-flawed Electronic Communications Privacy Act of 1986 and now contemplate an even worse law.

Section 9 of HR1674, the Cellular Amendment, was forged behind closed doors, without public access or public discussion, and released at Congressional recess prior to the end of the fiscal year as a coat-tail amendment to a vital piece of legislation--the FCC Funding Bill--all to avoid challenge.

Naturally there was no initial objection--no one knew about it. But a groundswell of objection to this special interest legislation is building rapidly, and the public is asking their legislators to act responsibly.

We are aware of the influence over our representatives wielded by the well-funded cellular lobby, but would hope that our legislators will listen this time to some facts as well as the marketing myths of the CTIA.

We urge the Senate to adopt--unamended--S1132, the FCC Funding Bill, and oppose Section 9 (Interception of Cellular Telecommunications) of the House version (HR1674) which would prohibit the manufacture of scanning radio receivers which include cellular telephone frequencies, for the following reasons:

(1) The FCC, who will be required to deny type acceptance to scanners with cellular frequency coverage, has gone on record opposing such measures, noting that these frequencies are shared with other services which may be freely monitored (GEN.Docket 88-281).

(2) Expert witnesses testifying at the ECPA hearings went on record stating that a ban on monitoring certain frequencies is totally unenforceable.

(3) Radio frequencies are "loaned" to services, often changing in time. Legislation against receiving a specific frequency is in direct conflict with the FCC's directive to reallocate spectrum as necessary to best serve the national interest.

(4) We already have one law prohibiting the monitoring of cellular conversations (ECPA, 1986), and another prohibiting the

divulgence or use of anything overheard on the airwaves (Communications Act, 1934). These existing laws are adequate to protect a reasonable expectation of privacy.

(5) The Bill's proponents claim it will "bring the FCC's equipment certification process in line with ECPA", which it will not. Quoting FCC GEN. Docket 88-281: "...the ECPA does not prohibit the manufacture and sale of scanners...based solely on the ability to receive specific frequencies."

Curiously, other ECPA-protected frequencies which carry stricter penalties than cellular listening are unaddressed by the proposed amendment, and shortwave radios which include ECPA-protected frequencies ar not being altered.

(6) The responsibility of privacy protection is on the sender, not bystanders. Quoting 89 F.C.C2d 450, 455: 1982, "...the initial responsibility for signal protection should be on the signal originator, who is in the best position to protect the signal against unauthorized interception and use." All users of the radio spectrum--except the mobile telephone companies--comply with this rule.

(7) CTIA's successful ECPA appeared to legitimize their false claim that cellular telephones were private instead of truthfully advising their customers that their conversations could be easily overheard.

Section 9 is a profit expedient designed to force scanner manufacturers to bear the cost of conforming to cellular's privacy illusion rather than cellular complying with the statutory obligation to protect their customers' privacy.

Effective scrambling is already available to customers who request that measure of privacy. Expecting the cellular industry to take simple measures to assure their customers privacy makes more sense than demanding the rest of the communications industry to change all of their products to accomodate the higher profit motivation of the cellular industry.

The successful passage of Section 9 will remove any incentive for the cellular industry to provide real privacy, forcing the public to accept the claim of fake, legislated privacy.

(8) Cellular has announced that it will be digitizing their communications within the next few years, making them unintelligible. During that period, existing cellular-capable scanners will still be operational. Section 9 accomplishes nothing.

(9) Even with the successful passage of the amendment, present and future tunable receivers, test equipment, TV sets, VCRs and frequency converters would still legally tune cellular frequencies.

Even cellular-censored scanners will readily receive, without modification, cellular "images", duplicates of the original signal in another frequency-range unaffected by the ban: Listeners cannot avoid hearing cellular communications while monitoring unprotected frequencies in those non-cellular ranges.

Our judicial system has historically held that ignorance of the law is no excuse: ignorance of the laws of physics is no excuse for Congress to implement inherently faulty legislation.

(10) Since the proposed legislation bars only manufacture and not sales, possession or use, it appears that cellular-capable scanner kits as well as home-made scanners would remain lawful."'.

(11) The Bill bans the manufacture of scanners 'that can be' "readily-altered" to receive cellular. What constitutes readily altered? Adding an external converter? In that case, no scanners of any type could be manufactured, since any one of them could be "altered" to receive cellular."

(12) Cellular telephones are like any other two-way radios; they broadcast radio waves for many miles. Consumer electronics equipment is notoriously vulnerable to radio signals; many non-scanner products--TVs, VCRs, portable radios--unintentionally pick-up cellular phone calls. The cheaper they are, the more vulnerable and pervasive they are in American households.

(13) The courts have continuously held that radio transmissions may have no reasonable expectation of privacy (U.S. v. Hoffa, 436 F.2d 1243, 7th Cir. 1970), and the laws of Congress will not change the laws of physics.

(14) A ban on cellular-capable scanners would deprive millions of licensees an inexpensive, reliable and legal way to monitor interference they may be causing to the cellular services, as well as determine whether interference they are experiencing may be caused by a cellular system (as allowed under the ECPA).

(15) The ban would deprive Part 15 users and Experimental Class licensees their legal access to inexpensive, readily-available receiving equipment for their authorized services.

(16) The term "cellular'* is generic, referring not only to radio telephones but any radio system which utilizes this technology. The wording of Section 9 would create a regulatory nightmare for Congress to resolve.

(17) Section 9 establishes a dangerous precedent by encouraging other licensees and special interest groups to demand equal protection by frequency censorship, inviting abuses of the spectrum to go unmonitored and unreported by conscientious listeners.

The FCC is unable now to police the airwaves, even before

frequency censorship. Virtually every. FCC investigation comes from outside monitoring, Section 9's restrictions would have a chilling effect on citizen-involved reporting and enforcement.

(18) One of the privileges historically accorded to U.S., citizens is public access to the airwaves, a right that would be den'ied with, a prohibition, against such; access.

The amendment accents a dangerous political.. precedent: totalitarian countries now have more listening- freedoms than Americans have,-

(19)One of the largest dealers reports that 90% of his cellular-capable scanners, all of which are manufactured in Asia, are sold to the U.S. government. Many others go to law enforcement agencies to gather. evidence during crimminal investigation.

With cellular coverage banned,. manufacturers would redirect their sales to other world consumer markets,: leaving no American alternative except exhorbitant laboratory instrument&,' seriously compromising legitimate investigation. Even these remaining. instruments are all large and heavy, depriving field agents of vital portability.

(20) Realistically, the& is no reason to expect such. a-scanner' ban to be any more effective than present restrictions against. uncertified CB radios, computers and' other contraband which is freely distributed in the United States.

Conclusion:
Cellular companies have an obligation to consumers to provide privacy; this can only happen with scrambling. Successful passage of Section 9 will deny such privacy, endorsing cellular's more profitable charade while eavesdropping continues unabated.

Until the cellular industry follows their statutory directive to protect the privacy of their customers, we would propose a simple, inexpensive and effective alternative amendment: Require all cellular telephones to carry a warning label cautioning the user that his conversations may be easily overheard.

February 1, 1993

Donna R. Searcy
Secretary, Federal Communications Commission
Room 222; 1919 M Street
Washinton, DC 20554

Ref. Docket 93-l

In accordance with the provisions for comment on pending FCC rulemaking, the following comments are submitted in response to ET Docket No. 93-1,. Amendment of Parts 2 and 15 to prohibit the Marketing of Radio Scanners Capable of Intercepting Cellular Telephone Conversations.

(1) A redefinition of a scanning receiver as described in CFR Title 47, Part O-19, section 15.3 (v) would read as follows:
For the purpose of this part, a scanning receiver shall be defined as a channelized VHF/UHF radio receiver specifically designed to allow the selective entry into multiple memory locations discrete radio frequencies without regard to numeric sequence or consistent spacing in the spectrum, and which automatically samples those memory locations in rotation for signals to be monitored. Receivers intended for operation as part of a licensed station are not included in this definition.

(2) A definition of a scanning receiver capable of "readily being altered by the user" (Docket proposal, paragraph 5 and 7) would be one which accomodates the installation into its existing internal circuitry an additional, readily-available component: or which accomodates the simple expedient of removing, replacing or cutting an internal circuit component, and which can be accomplished by a person who possesses minimal technical knowledge.

(3) The prohibition against scanners "being equipped with decoders that convert digital cellular transmissions to analog voice audio" is redundant and unnecessary. If the scanner cannot receive cellular transmissions, then it cannot provide analog audio from such transmissions.

In addition, no manufacturer can, in good faith, certify that its scanner cannot be equipped with a digital to analog coverter. The FCC is forcing manufacturers to perjure themselves to do business.

(4) While purporting to be responding to the Telephone Disclosure and Dispute Resolution Act and the Electronic Communications Privacy Act, the Commission actually exceeds the bounds of its Congressional directive by proposing a ban on frequency converters which are not, in fact, opposed in either Act.

Designing and manufacturing a frequency convertor for the legitimate reception of 806-960 **MHz** amateur, public safety, experimental and other unprotected services, yet which does not respond to signals in the cellular frequencies, is not feasible.

By banning frequency converters the Commission invents an unjustified and repressive rulemaking which will stifle many small American businesses who depend upon the marketing of such legitimate accessories during this sensitive period of American electronic recovery.

Respectfully,

Bob Grove
President, Grove Enterprises
Publisher, Monitoring Times

EXHIBIT
E

Federal Communications Commission

Report to Congress

on

AVAILABLE SECURITY FEATURES FOR PROVIDING CELLULAR TELEPHONE PRIVACY

June 1, 1993

PREFACE

This report is provided in compliance with Section 403(b) of the Telephone Disclosure and Dispute Resolution Act (Pub. L. 102-556, 106 Stat. 4181). This Act required the Federal Communications Commission to adopt rules prohibiting the manufacture and import of scanning receivers capable of eavesdropping on cellular radio signals. Further, this Act requires the Commission to report on available security features for both analog and digital cellular radio signals, along with cost information on such features.

INTRODUCTION

This report responds to **Section** *403* of the Telephone Disclosure and Dispute Resolution Act (TDDRA), Pub. L. 102-556. Section 403 requires the Federal Communications Commission to prescribe regulations denying equipment authorization for certain scanning receivers capable of receiving cellular radio communications; and, report to Congress by June 1, 1993, on available security features for both analog and digital cellular radio signals.

In this report, we first summarize the provisions of the TDDRA and the Commission's actions to adopt rules prohibiting scanning receivers in accordance with the TDDRA. We then briefly describe how cellular radio systems operate and how eavesdropping on cellular communications occurs. We next provide an overview of the techniques currently available to impede eavesdropping for the current analog cellular system. Information on the cost of these technologies is included, as requested in the TDDRA. Finally, we discuss the development and implementation of new digital cellular technology that is expected to be significantly more resistant to eavesdropping than the current cellular technology.

TELEPHONE DISCLOSURE AND DISPUTE RESOLUTION ACT

On October 28, 1992, the President signed the TDDRA into law. Paragraph (a) of Section 403 of this Act adds a new Section 302(d) to the Communications Act of 1934 (47 U.S.C. Section 302). New Section 302(d) requires that by April 26, 1993 (180 days after enactment of the TDDRA), the Commission prescribe and make effective regulations henying equipment authorization for any scanning receiver that is capable of:

> receiving transmissions in the frequencies allocated to the domestic cellular radio service,
>
> readily being altered by the user to receive transmissions in such frequencies, or
>
> being equipped with decoders that convert digital cellular transmissions to analog voice audio.

Further, new Section 302(d)(2) provides that, beginning one year after the effective date of the regulations adopted pursuant to paragraph (d)(l), no receiver having such capabilities shall be manufactured in the United States or imported for use in the United States.

As defined in the Commission's rules, scanning receivers, or "scanners," are radio receivers that can automatically switch between four or more frequencies anywhere within the 30-960 MHz band.[1] In order to control their potential to cause harmful interference to

---

[1] See 47 *CFR Section 15.3(v).*

authorized radio communications, the Commission's rules require that scanners receive an equipment authorization (certification) from the Commission prior to marketing.* The Electronic Communications Privacy Act of 1986, Pub. L. 99-508, in part, made it illegal to intentionally intercept cellular communications or to manufacture equipment primarily useful for the surreptitious interception of cellular communications.[3] However, the Commission was not given specific authority to deny equipment authorization to scanners that receive cellular frequencies. As a result, such scanners have been routinely authorized by the Commission.'

In response to the TDDRA, on January 4, 1993, the Commission adopted a ***Notice of Proposed Rule Making*** in ET Docket No. 93-1, proposing to deny equipment authorization to scanning receivers that: 1) tune frequencies used by cellular telephones; 2) can be readily altered by the user to tune such frequencies; or, 3) can be equipped with decoders that convert digital cellular transmissions to analog voice audio.' The ***Notice also*** proposed to deny equipment authorization (notification) to frequency converters that tune, or can be readily altered by the user to tune, cellular telephone frequencies.[6] To assist the Commission in determining compliance with these requirements, it was proposed that applicants for certification of scanners, and for notification of frequency converters used with scanners, be required to include in their applications a statement stating that the device cannot be easily altered to enable a scanner to receive cellular transmissions.

---

[2] See 47 ***CFR Sections 15.101 (a) and 2.1031 et seq.***

[3] See 18 *U.S.C.* Sec. 2.511, 2512.

[4] ***In the past five years, 22 different models of scanning receivers capable of receiving cellular telephone transmissions have been issued grants of equipment authorization by the Commission. During this same period, ten other models capable of tuning frequencies benveen 806 and 900 MHz except for the cellular bands have also been authorized. Several publications currently on the market describe relatively simple modifications that users can make to many of the latter scanning receivers to enable that equipment to receive cellular telephone transmissions.***

[5] ***See Notice of Proposed Rule Making in ET Docket No. 93-1, adopted January 4, 1993, 8 FCC Rcd 359 (1993).***

[6] ***There arc a number of frequency converters on the market that convert cellular radio transmissions in the 800 MHz band to lower frequencies. These devices can be easily used in conjunction with scanners that receive frequencies below 800 MHz to enable the reception of cellular relephone transmissions. These converters are receivers subject to authorization under the notification procedure, as described in Section 15.101 of rhe FCC rules (47 CFR Section 15.101).***

Forty six parties filed comments on the *Notice* and six parties filed reply comments. A large number of commenters, presumably most of them scanner enthusiasts, opposed adoption of any rules that would restrict the tuning capabilities of scanners. Manufacturers of scanners, and cellular service providers, in general supported the Commission's proposed changes while suggesting a few minor modifications.

On April 19, 1993, the Commission adopted a *Report and Order* in ET Docket No. 93-1, implementing regulations that prohibit the manufacture or importation of scanning receivers capable of tuning cellular radio frequencies in accordance with the TDDRA.[7] The regulations provide as follows:

> the manufacture or importation of cellular scanning receivers capable of receiving cellular frequencies must cease as of April 26, 1994;
>
> no such scanning receivers will be authorized by the Commission after April 26, 1993;
>
> frequency converters that tune cellular frequencies are treated in the same way as scanning receivers;
>
> for scanning receivers that tune frequencies outside the cellular frequency bands, the manufacturer must confirm, as a condition of FCC equipment authorization, that the equipment cannot be readily altered by the user to receive transmissions in cellular frequency bands;
>
> and, scanning receivers must be incapable of converting digital cellular transmissions to analog voice audio.

Paragraph (b) of Section 403 of the TDDRA states that the Commission shall report to Congress no later than June 1, 1993, on available security features for both analog and digital radio signals. This report is to include a study of security technologies currently available, as well as those in development. This study shall assess the capabilities of such technologies, the level of security afforded, and cost associated with wide-spread deployment of such technologies.

HOW A CELLULAR TELEPHONE SYSTEM WORKS

In order to understand how it is possible to eavesdrop on a cellular telephone conversation, and ways to inhibit eavesdropping, it is first necessary to understand the basic principles of

---

[7] *See Report and Order in ET Docker No. 93-1, adopted April 19, 1993, FCC Rcd (1993).*

operation of cellular systems. Cellular telephone systems provide access to the Public Switched Telephone Network (PSTN) using radio frequency links between mobile phones and a network of radio base stations, as shown in Figure 1. The operating area served by each base station is called a cell. Each cell is assigned a set of operating frequencies by the service provider.

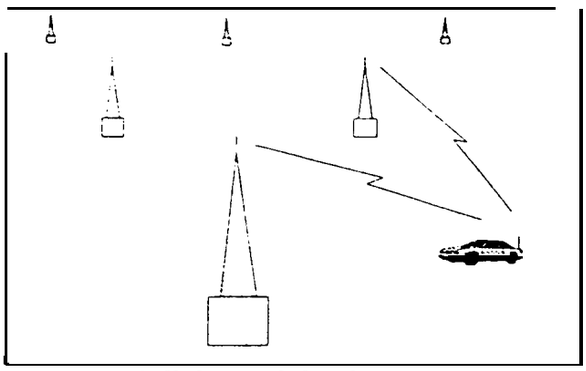

Figure I: Cellular mobile phones are connected to the PSTN through a nenvork of base stations.

Figure 2 illustrates how cellular systems achieve a high degree of spectrum efficiency through reuse of frequencies in the network of cells. Two fundamental principles are applied in assigning frequencies to each cell:

The frequencies assigned to two adjacent cells must be different to avoid interference.

Frequencies may be reused two cells away.

When it is necessary to increase communications capacity, large cells are split into smaller cells by reducing base station transmitter power and adding new base stations. Frequencies are reused in the smaller cells by applying the above principles.

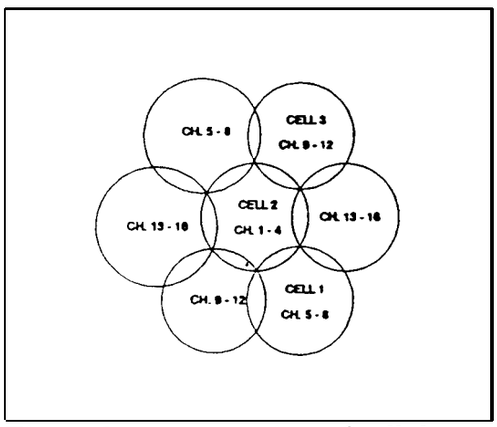

Figure 2: Overhead view of cellular nenvork showing how adjacent bare stations ("cells") use different communication channels.

At the heart of the cellular system is a highly-complex computer switch. The switch performs several functions:

It determines which of the base stations will be used to communicate with the mobile unit.

It instructs the mobile unit to tune to the frequencies that will be used for each particular conversation.

It connects each call to the PSTN.

The cellular switch is able to carry out the above functions dynamically. This enables the cellular network to "hand-off' calls from one cell to the next in mid-conversation as the mobile unit moves about the service area. (See Figure 3.) Since no two adjacent cells are assigned the same base station frequencies, a hand-off always results in a change of operating

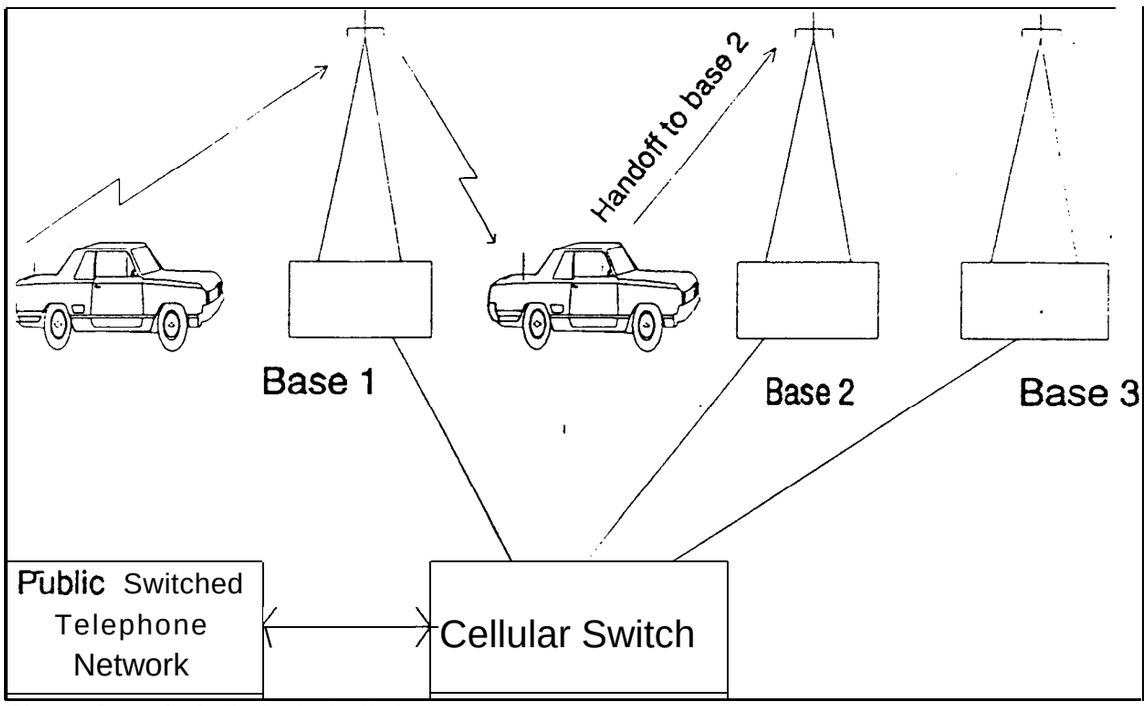

Figure 3: A basic cellular telephone system.

frequency. The hand-off from one cell to the next is transparent to the user.

The Commission licenses two cellular service operators in each s&vice area. Cellular service areas typically encompass metropolitan areas or major highway routes in rural areas. One license is assigned to the local wireline common carrier; the second license is assigned to a competitor. Non-wireline licenses may be sold, and today, carriers have purchased the non-wireline licenses in many service areas to offer wide-area contiguous service.

Each cellular licensee is provided 25 MHz of spectrum, for a total of 50 MHz of spectrum available for cellular service in each service area. The cellular frequency bands are 824-849 MHz for mobile transmitters and 869-894 MHz for base transmitters.

Table 1 lists the cell, channel and frequency statistics of a cellular system. The 50 Mhz of cellular spectrum is divided into 1,664 channels that are spaced 30 kHz apart. Since two-way conversation requires two channels, this translates to 832 two-way, or duplex channels. Forty-two duplex channels are used for cellular network control purposes, such as for initial

Frequency Bands	824-849 MHz, 869-894 MHz
Channel Spacing	30 kHz
Control Channels per system	21
Communication Channels per system	395
Maximum Communication Channels per cell	57
Typical Cell Size	20 km maximum diameter; 4 km minimum diameter.

Table I: Cellular system spectrum usage. The Commission authorizes nvo cellular systems in each service area.

call set-up, leaving 790 duplex channels available for communications. Since two cellular systems can be assigned to each market, 395 duplex communications channels and 21 control channels are assigned to each system. A typical cellular system uses a 7-cell frequency re-use pattern resulting in 395/7 = 56.4 communications channels per cell. In other words, up to a maximum of 57 conversations may by held simultaneously in any given cell.

Several factors are taken into account in establishing cell sizes. One important factor is the power limitation of the mobile unit. For example, operations with battery powered hand held units are not possible in some areas of large cells. Another important consideration is the distribution of service demand across the service area. High density areas require more cells to meet high communications traffic demand. Another factor is costs: base stations cost up to $1 million to construct.*

The cell size is determined by the power of the base station transmitter. Typically, cells are no larger than about 20 kilometers (12 miles) in diameter and no less than about 4 kilometers (2.5 miles) in diameter. As a cellular system matures, large cells are gradually split into smaller cells to accommodate the increase in communications traffic due to subscriber growth. For instance, a system may begin service with about 10 cells and eventually grow to 50 or more cells through cell splitting.

---

[8] ***Neil J. Boucher, The Cellular Radio Handbook, (Mendocino, California: Quantum Publishing, inc., 1990), pp. 346-347.***

CELLULAR SCANNING RECENERS

The advances in microelectronics and receiver design that occurred in the 1970s made it practical to develop consumer FM scanning receivers capable of tuning hundreds of radio channels. Scanning receivers include a microprocessor that can be programmed by the user to monitor specific radio channels. These receivers generally differ by the radio communication frequency bands they can tune and their degree of programmability. Most are designed to cover the mobile communications frequency bands used for police, tire, aeronautical, maritime, and business communications. Some include coverage of the cellular radio frequency bands. Scanning receivers typically sell on the retail market for $ 100 to $300, and are available in retail stores throughout the United States.

Scanning receivers have the potential to generate radio noise and therefore possibly to interfere with radio communications services. To ensure compliance with standards designed to control radio interference, the Commission requires that all scanning receivers comply with its equipment authorization procedures prior to being marketed. In the past five years the Commission has authorized 22 scanning receivers capable of tuning the cellular frequencies. An additional 10 units have been authorized that tune to frequencies near the cellular frequency bands; these units can probably be modified by the user with minimal effort to tune the cellular frequency bands. Manufacturers are not required to report sales figures to the Commission and we are unaware of any reliable sales estimates.

HOW EAVESDROPPING OCCURS

Eavesdropping on cellular telephone conversations is a violation of the Electronic Communications Privacy Act of 1986.[9] However, it is extremely difficult to detect the act of interception, thereby posing challenges for enforcement efforts. From a technical standpoint, several factors make it easy to monitor cellular conversations. While some characteristics of cellular system operations do pose impediments to monitoring of a specific individual or conversation, there are ways they can be overcome.

Almost all current cellular radio operations employ unencrypted, standard analog FM modulation." A simple FM receiver that can tune to the cellular frequencies is all that is required to listen to cellular telephone conversations that are transmitted using standard FM

---

[9] *See Electronic Communications Privacy Act of 1986, Pub. L. 99-508.*

[10] *FM modulation is the same technique used in FM broadcasting, as well as the audio portion of TV signals and most other business, police, and fire mobile communications equipment.*

modulation. More sophisticated devices such as scanning receivers make it possible to quickly locate, and eavesdrop on, occupied cellular channels.

While there are nearly 800 cellular two-way voice channels available for cellular systems in a service area, as noted earlier only a fraction are used in any given cell. This reduces the number of channels that may be used at any given location to about one hundred. A scanning receiver can quickly scan through all the channels, identify the ones in use at a particular location, and be programmed to monitor those channels. The scanner will tune through each of the channels programmed by the user and stop whenever it detects a conversation. The user can decide whether to listen to the conversation, or skip to another channel.

The fact that the cellular system selects the cells and frequencies to be used for a given telephone call and hands-off the call from one cell to another makes it difficult to eavesdrop on a specific individual or conversation. However, these impediments can be overcome to some degree. For example, if the location of the individual to be intercepted is known, it is easy to determine which cell is likely to be used and, with proper research, the frequencies available at that cell. If the cellular user's conversation is occurring in a large cell, there is less likelihood of a hand-off. Further, hand-offs can be dealt with somewhat by following the mobile cellular user as he or she moves about the cellular service area. To better increase the chances of eavesdropping on a particular conversation, multiple scanners and audio recorders might be used.

More advanced monitoring techniques are also possible. With the proper equipment, an eavesdropper could monitor cellular control channels to obtain the identification number of a particular cellular radio user. This would enable the eavesdropper to track a particular call through the cellular system.

Of course, commercial radio service equipment is available that is technically capable of monitoring and tracking specific cellular conversations. Further, we are aware that it is possible to program standard cellular mobile radios through the alpha/numeric keypad to tune to any cellular channel. Such programmability is necessary for servicing and repairs. At this time, it does not appear necessary or appropriate to control the availability of radio service equipment covering the cellular frequency bands or the programmability of cellular radios. To do so would greatly impede servicing of cellular systems and equipment.

SECURITY FEATURES FOR ANALOG CELLULAR SYSTEMS

The current analog cellular technical standard has its roots in technology developed more than 20 years ago and was never envisioned to be voice-secure so as to preclude eavesdropping. At that time, low-cost scanning receivers capable of tuning cellular frequencies were not even on the horizon, so the developers of the analog standard had no reason to make it voice-secure.

Voice security for the current analog cellular systems has only recently received significant attention. In the last few months, several manufacturers have announced voice security products for analog cellular systems. The consumer products that they are offering scramble the voice portion of a cellular signal using a variation of an encryption technique called "frequency inversion." In a frequency inversion system (see Figure 4) the audio frequencies being transmitted (typically voice) are inverted around a split frequency, resulting in a sound that is virtually unintelligible to an ordinary receiver. A frequency inversion system typically switches the high and low frequencies in a transmission. This unintelligible audio signal is then fed into a cellular transmitter, transmitted through the air, and inverted again at the cellular receiver. A second inversion, at the receiver, restores the audio signal to its original form, making it once again intelligible.

A simple frequency inversion system where the same split frequency is constantly being used is relatively easy to decipher. Moreover, it can reduce operating range by as much as 60 percent.*' This reduction in operating range leaves gaps between cells where the user is unable to obtain satisfactory service. The service provider can compensate for these gaps in coverage by adding more cells, but the cost of each new cell can easily exceed $1 million. Because of these factors, simple frequency inversion systems have gamed little support from the cellular industry in the past.

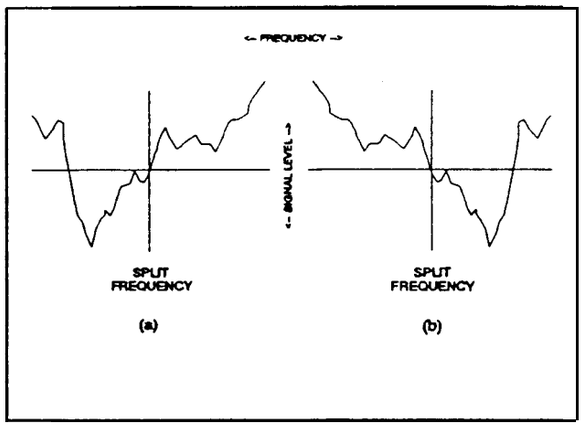

Figure 4: A voice audio signal (a) and its inverted counterpart (b).

The.new encryption products currently on the market have improved on simple frequency inversion by using sophisticated electronic circuits to change the split frequency being used many times per second using a randomly generated code known only to the cellular transmitter and receiver. This procedure makes it much more difficult for an eavesdropper to decipher the transmitted signal. Also, because more elaborate filters are required at the receiving end of the encrypted signal to keep up with the changing split frequency, the ability of the receiver to distinguish between extraneous noise and the actual cellular signal is significantly improved, thus minimizing the loss of coverage range. The enhanced capabilities in the mobile radios does, however, increase the cost of these units.

Cellular telephone encryption systems can be provided by cellular operators as a service to their customers. They can also be provided by end-users, or third parties, independently of cellular operators.

---

[11] *Boucher,* ***p. 432.***

Encryption service provided by cellular operators. AT&T has announced that they are introducing the "AT&T Advanced Cellular Privacy System." It consists of encryption equipment installed at the cellular operator's switch and in portable and mobile phones. According to AT&T, this system uses a combination of frequency inversion and time scrambling to encrypt the over-the-air signal so that anyone intercepting it will hear only a chirping sound. The cost to consumers of mobile phones that incorporate this encryption technology can range from $600-$700 (for an AT&T privacy module that adapts to a variety of mobile and transportable phones) to $1,300-$1,500 (for an AT&T portable phone that includes built-in encryption circuitry). This compares to current cellular mobile and portable unit costs of $300-700.[12] In addition, users can expect to pay a monthly "subscriber" fee to the cellular service provider of somewhere between $10 and $20. The cost to cellular operators of the most basic configuration of encryption equipment installed at the switch is expected to be about $52,000. This minimum configuration would provide encryption for 24 T1 channels, (that is, 24 simultaneous cellular phone conversations) within the cellular system where it is installed.

The main advantages of the AT&T system are that 1) the level of privacy is very high because the system scrambles the signal in both the frequency and time domains; and, 2) it provides encryption of the over-the-air portion of the cellular phone conversation no matter who is the other party to the conversation. Its main disadvantage is that it may not provide privacy protection when the user is "roaming," i.e., out of range of a carrier with the encryption equipment installed in its switches. This short-coming is alleviated in some cellular systems where carriers with contiguous markets join to offer a "seamless" service by "sharing" subscriber data and billing.

Several other companies have also developed encryption systems for installation at cellular switches. PrivaFone Corporation of Towson, Maryland markets a system that operates in a manner similar to the AT&T system described above. PrivaFone's mobile encryption equipment can be used with most mobile phones. The PrivaFone mobile equipment costs approximately $700 to $1000, in addition to the cost of a conventional cellular mobile unit. A monthly service charge for encryption is also added by the cellular operator and runs between $10 and $20. The cost to cellular service providers of the most basic configuration of PrivaFone equipment is about $20,000. This minimum configuration provides encryption for 12 T1 channels (12 simultaneous cellular phone conversations) within the cellular system where it is installed.

Encryption service provided by end-users or third parties. Some companies are developing cellular voice security techniques that do not require modification of the cellular system. One such system, for example, is PrivaFone's Line Privacy Unit that can be

---

[12] *Mobile units are also available at significantly lower prices where the consumer also accepts a contract for service with a cellular operator for a specified period of rime, usually one year.*

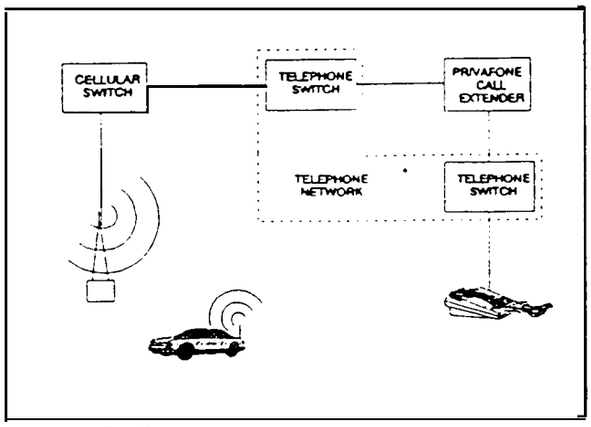

Figure 5: The PrivaFone system encrypts cellular calls independent of cellular service providers, and without the need for encryption equipment at the non-mobile phone.

installed at an office switchboard. Mobile phone users must be equipped with an add-on PrivaFone unit. Mobile users place calls to their office switchboard through the Privacy Unit (an encryption/decryption device) to get an outside line. If the call through the outside line is to another cellular mobile unit that does not use encryption technology, however, that link of the call will not be protected. PrivaFone's office unit retails for about $1000. Because the cellular service provider is not involved in this encryption scheme, there is no monthly encryption charge.

Safecall Inc. of Wethersfield, Conn., plans to offer a similar device for $600 that can be plugged into cellular phones. However, under Safecall's approach, the device would scramble a call and automatically dial a switchboard over a toll-free number. The switchboard would unscramble the signal and relay the call over the landline telephone network. Customers would pay $5 a month as well as 95 cents a minute, in addition to the normal cellular charges.

SECURITY FEATURES FOR DIGITAL CELLULAR SYSTEMS

As indicated above, almost all cellular phone networks today use analog transmitting equipment. However, several factors are driving cellular systems to implement new digital cellular technology. The main advantage of digital cellular technology is an increase in system communications capacity due to the robustness of digital signals and availability of signal processing techniques including audio compression. Increases in capacity are needed to accommodate the growing number of cellular subscribers, particularly in major metropolitan areas. Higher system capacity offers consumers better service by reducing the likelihood that a call will be blocked from access to the network.

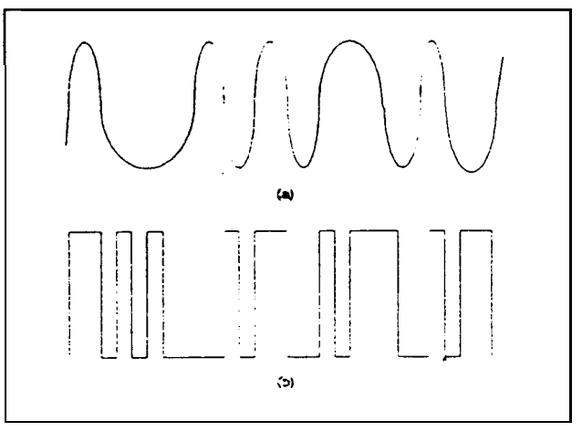

Figure 6: An analog cellular radio signal (a), is convened to a digital cellular radio signal (b) -- a stream of pulses representing the computer language of 1s and 0s.

Digital technology also offers improved performance features, such as voice security and improved compatibility with landline digital networks for transmission of facsimile and personal computer data.

Digital radio techniques convert analog signals, such as voice, into a stream of digital pulses that represent Is and Os, as shown in Figure 6. The stream of Is and Os is encoded by a microprocessor and then is used to modulate a radio transmitter. The digital pulses sound like hiss when listened to over-the-air with conventional radio receivers. A receiver that has a microprocessor that can properly decode the digital pulses is used to recover the original audio signal. The coding and decoding occur virtually instantaneously and without the knowledge of the user. The microprocessor can be programmed in very sophisticated ways so that it is extremely difficult for an eavesdropper to decipher the voice signal.

In 1988, the Commission amended its rules to enable cellular operators to offer digital and other new technologies in the cellular frequency bands if they choose to do so.[13] This flexibility was conditioned on the cellular operator continuing to provide an appropriate quality of service to analog users.

The Telecommunications Industry Association (TIA), which is composed of cellular equipment manufacturers, working in conjunction with cellular service providers under the auspices of the Cellular Telecommunications Industry Association, in May 1990, adopted an interim standard IS-54 for digital cellular systems.[14] This standard is based on use of a technique called Time Division Multiple Access (TDMA). In TDMA each of the voice signals is digitized and compressed to take up less time. The compression is accomplished by removing the "dead air" time in conversations. The digitized signals can then be assigned time slots for transmission. Each cellular TDMA transmission uses the same 30 kHz of bandwidth as an analog FM transmission. A TDMA signal is illustrated in Figure 7.

The IS-54 standard includes capability for sophisticated voice encryption. In fact, use of the encryption technique employed in this standard required approval by the National Security Agency. The degree of security provided by this and other digital communications technologies has received considerable attention from the Federal Bureau of Investigation and the National Security Agency in the past two years because of their concern that digital techniques will greatly impede legal wiretapping and monitoring for law enforcement purposes. [15][16]

---

[13] *See Report and Order, General Docker No. 87-390, 3 FCC Rcd 7033 (1988). See also* 47 *CFR Section 22.930.*

[14] *See EIA/TIA Interim Standard, IS-54, Cellular System Dual-Mode Mobile Station - Base Station Compatibility Stondard.*

[15] *Sessions, William S., "Keeping an Ear on Crime," The New York Times, March 2 7, 1992. p. A35.*

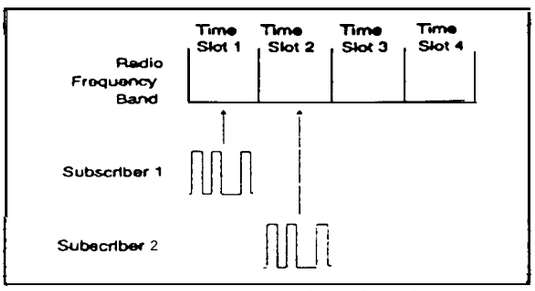

Figure 7: In TDMA each subsriber signal is digitized and assigned a time slot for transmission. Since the time slots are assigned irregularly, it is difficult to 'decode' a panicular subscriber conversation.

The voice security feature of IS-54 will be incorporated in the new generation of dual-mode (analog - digital) mobile units and is expected to be offered by cellular system operators as an optional service. The standard calls for use of a 528-bit field consisting of two 260-bit masks for voice privacy on a digital traffic channel. One mask is for speech transferred from mobile to base; the other from base to mobile. The masks are calculated using a digital bit stream that is generated during call set-up. This bit-stream is partially random for each call. While no security system can be considered fool-proof, it appears that the IS-54 standard provides a high level of security protection.

TIA is developing a second digital cellular standard based on a technology called Code Division Multiple Access (CDMA). CDMA is a form of spread spectrum communications, a technique long used by the military for secure communications. With CDMA, as illustrated in Figure 8, the digitized voice signal is mixed with a randomized code sequence that is unique to each mobile unit. The combined digital signal modulates the transmitter'in such a way as to produce what appears to be radio noise. CDMA signals are very wide -- typically one to ten megahertz -- as compared to TDMA or the current analog cellular signals. CDMA signals are nearly impossible to detect unless a receiver is used that has the proper decoder and is programmed with the correct code sequence. Considerable debate and study is under way in the cellular industry as to whether TDMA or CDMA provides greater improvements in system capacity and quality of service at the most economical cost.

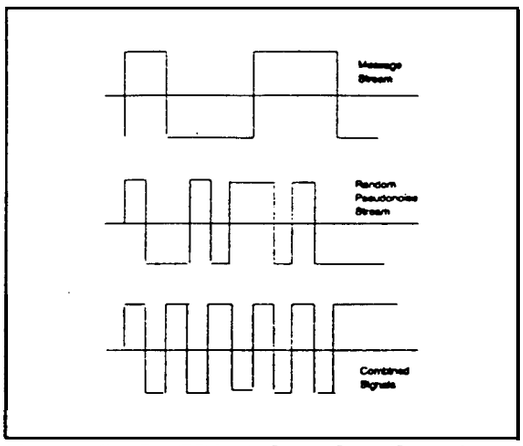

Figure 8:. In CDMA the subscriber signa is digitized and then added to a random digital signal. This makes the combined signal difficult to decode without the 'key.'

[16] *Markoff, John, "New Cellular Phones Raise A National Security Debate," The New York Times, February 6. 1992, p. D1.*

Digital systems have only just begun to be put into operation. McCaw Cellular Communications announced on March 18, 1993, that service on the first all-digital cellular system in the United States has been initiated in South Florida. Southwestern Bell Mobile Systems also announced, on the same day, a 4,000-customer trial of its digital system in Chicago, to be followed later this year by digital service throughout its entire Chicago system. Both of these systems employ TDMA technology.

Qualcomm has been testing cellular systems that use CDMA technology in conjunction with Bell Atlantic, Ameritech, GTE, U.S. West and other cellular service providers. Currently, PacTel is operating an experimental CDMA system in San Diego. It is expected that, by the end of next year, full commercial operation of cellular networks that use CDMA technology will have begun in some U.S. cities.

It is generally anticipated that digital technology will be implemented widely in cellular systems. However, cost issues are likely to affect the timing. Currently, digital cellular mobile units cost approximately twice as much as analog models. There is also the substantial costs of converting the base station transmission equipment. Outside of major cities, there may be little need of, or benefit from, increased system capacity. However, this could change as new types of data services are introduced over cellular systems. The pace of digital conversion may lie in the hands of subscribers and their demand for the technology.

CONCLUSIONS

Most cellular telephone calls today are relatively easy to intercept because they are broadcast over-the-air as analog, unencrypted FM radio signals. This situation is expected to change in the future. First, the recently adopted prohibition on manufacture and importation of scanning receivers that can tune cellular frequencies, should stem the tide of equipment available for eavesdropping. Second, voice-secure equipment is becoming available for the current analog cellular systems. Finally, new digital cellular technology that will greatly increase the difficulty of eavesdropping on cellular telephone conversations is beginning to be implemented and may well ultimately resolve this problem.

Experience has shown that no encryption technique is fool-proof. At best, all one can do is try to make decryption extremely difficult and expensive. Because the solution to cellular eavesdropping will come from technological development and deployment, further legislative or regulatory action would not likely ameliorate the current situation. However, to the extent encryption technology improves and abuses nevertheless persist, legislative or regulatory action might then be advisable.

BIBLIOGRAPHY

Altschul, hlichael, Cellular Telecommunications Industry Association letter dated April 13, 1993, responding to FCC request for information on voice security features for cellular telephones..

Boucher, Neil J., *The **Cellular Radio Handbook.*** Mendocino, California: Quantum Publishing, Inc., 1990.

Calhoun, George, ***Digital Cellular Radio.*** Norwood, Massachusetts: At-tech House, Inc., 1988.

"Cellular '93 Focus: Digitization, Data, Safety," ***Advanced Wireless Communications,*** March 3, 1993.

Cooper, Martin, "Want Digital Sooner? Offer Some Real Solutions," ***Telephone Engineering & Management,*** March 1, 1993.

Eckert, K. D., "Conception and Performance of the Cellular Digital Mobile Radio Communication System CD 900," ***Proceedings of the 37th IEEE Vehicular Technology Conference,*** Tampa, June 1-3, 1987, pp. 365-377.

EIA/TIA (Electronic Industries Association/Telecommunications Industry Association) ***Interim Standard IS-54: Cellular System Dual - Mode Mobile Station - Base Station Compatibility Standard, May 1990,*** published by Electronic Industries Association, 2001 Pennsylvania Ave., N.W., Washington, D.C. 20006.

Faulkner, Michael and Villani, Giovanni A., "Noise Reduction in Single Channel Radio Bearers Employing Privacy," ***IEEE Transactions on Vehicular Technology, Vol. VT-34, No.*** 3, August, 1985.

Halpem, Samuel W., "Introduction of Digital Narrowband Channel Technology into the Existing Cellular Spectrum in the United States," ***Proceedings of the 37th IEEE Vehicular Technology Conference,*** Tampa, June l-3, 1987, p. 149.

Jiang, Tongze, "A Comparison between the Three Mobile Digital Communications Systems," ***Proceedings of the 37th IEEE Vehicular Technology Conference,*** Tampa, June 1-3, 1987, pp. 359-362.

Jones, Lawrence R., & Salmasi, Allen, "The Cellular Semi-Finals," ***Telephone Engineering & Management,*** June 1, 1992.

Lee, William C. Y., *Mobile Communications Design Fundamentals*, Indianapolis: Howard W. Sams, 1986.

Markoff, John, "New Cellular Phones Raise A National Security Debate," *The New York Times,* February 6, 1992, p. D1.

Mikulski, James J., "DynaT*A*C Cellular Portable Radiotelephone System Experience in the U.S. and UK," *IEEE Communications Magazine,* Vol. 24, No. 2, February, 1986, pp. 40-46.

Nuggehally, S. Jayant, et al., "A Comparison of Four Methods for Analog Speech Privacy," *IEEE Transactions on Communications, Vol. Corn-29, No. 1*, January, 1981.

Personal Communications Technology, "Metropole Charges Southwestern Bell with Interception of Cellular Transmissions," December 1986, p. 30.

Quigley, Philip J., "The Privacy Loophole: How Technology Leapfrogs the Law," *Personal Communications,* October 1985, p. 29.

Schimmel, Eric J., Telecommunications Industry Association response of April 30, 1993, to FCC request for information on voice security features for cellular telephones.

Sessions, William S., "Keeping an Ear on Crime," *The* New York *Times*, March 27, 1992, p. A35.

Shosteck, Herschel, "Rumors of Analog's Death Have Been Greatly Exaggerated," *Telephone Engineering & Managemenr*, March 1, 1993.

Cellular phone firms blast Burris' opinion

Chicago Tribune, Wednesday, March 30, 1994

Exhibit F

By Andrew Gottesman
TRIBUNE STAFF WRITER

Tribune photo by Carl Wagner
Atty. Gen. Roland Burris says cellular-phone eavesdropping is legal under state law.

The cellular telephone industry reacted sharply Tuesday to Illinois Atty. Gen. Roland Burris' statement that using a police scanner to eavesdrop on cellular or cordless telephone calls is legal under state law because callers have "no reasonable expectation of privacy."

That's because eavesdropping oncellularcallshasbeenafederal crime since 1986, according to industry officials and legal experts.

Monday's legal opinion by Burris said eavesdropping on such calls was not prohibited by the state. But Burris' opinion, which serves as a guide for Illinois prosecutors, neglected to point out the federal ban.

On Tuesday, the Cellular Telecommunications Industry Association in Washington issued its own firm opinion about the matter.

"As an industry, we are totally committed to the personal privacy of cellular telephone users," the association's statement said "Cellular was never meant to be a 'broadcast-type' service, like CB radios, but rather, wireless telephony. The same expectation of privacy enjoyed by all Americans on the traditional wired phone network should apply to cellular."

Evan Richards, vice president of Personal Communication Systems at Chicago-based Ameritech, said the 1986 law came into being precisely because Congress thought customers had a right to expect privacy.

"I think this opinion gives you the feeling that you can't trust your phone, and that's not the case," he said.

So why would Burris issue such an opinion?

"We weren't asked about federal law," said Emie Slottag, a spokesman for Burris. "We were asked about Illinois law."

Cellular phones, such as car telephones, operate within a network such as Ameritech or Cellular One. Cordless phones are low-powered radios, transmitting to base units in the home. Both use normal radio waves, and therefore are subject to eavesdropping by relatively inexpensive devices such as a police scanner, which are commonly used by hobbyists.

Cordless phones are not covered under the 1986 federal law, mainly because they an? simply too easy to overhear on a scanner. Still, anybody trying to eavesdrop on a cordless conversation needs to be nearby..

In effect, the attorney general's opinion changes little, because eavesdropping on cellular communications has been illegal under U.S. law and eavesdropping on cordless communications never has been prohibited.

Burris was responding to a very narrow question when he issued his opinion Monday.

Jersey County State's Atty. Richard Ringhausen had asked Burris if an Illinois law prohibits somebody from recording a cellular or cordless conversation received over a police scanner. Burris. without addressing federal law, answered that the state statute does not carry such a prohibition.

David Strauss, a professor of law at the University of Chicago, said that states don't automatically outlaw everything prohibited by the federal government. It's not illegal under Illinois law, for example, to counterfeit U.S. currency. he said.

In any case, the legal rulings are becoming more and more moot. Digital technology now allows cellular and cordless customers to scramble their signals, so eavesdroppers just get a fax-like tone.

And a 1992 law, making it illegal to manufacture or import scanners that can pick up cellular frequencies, goes into effect Friday.

JACK SVETLIK

Man indicted in sport card theft